Anno 3 – N. 51
20 Maggio 2004 - 3 Giugno 2004

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

Direttore Responsabile: Luca Sprea

I Ragazzi della redazione europea: Bismark.it, Il Coccia, Gualtiero Tronconi, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron
Contents by MDR

Service: Cometa s.a.s.

DTP: Davide "Fo" Colombo

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Daniele Festa

Publishing company:
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing:
Roto 3

Distributore:
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti:
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

editoriale

Symantec e l'olio di serpente

Ragazzi, ragazze: siamo criminali. Tutti. Colpevoli di fare voce e contenuti al sito http://www.hackerjournal.it. Che è un sito criminale! Mica siamo noi a dirlo: è Symantec, attraverso il suo sedicente Norton Internet Security 2004 Professional, la cui funzione di controllo genitori blocca la navigazione del nostro sito. Categoria di blocco: crimine. Ovviamente Symantec non ha colpa, ehm, non sa quello che fa. Il suo software di controllo genitori (che serve a controllare appunto i genitori, in modo che spendano) dovrebbe bloccare i siti che contengono materiale pericoloso per i bambini, o qualcosa del genere. Invece non fa che guardare all'interno di una lista contenente una serie di parole tipo, per dire, hacker. Molto probabilmente, se ci chiamassimo Lamer Journal, potremmo essere pieni della peggiore immondizia ma per Symantec andrebbe tutto bene. Se ci chiamassimo Sasser Journal e facessimo i distributori di virus potremmo spargere il panico per qualche giorno e qualche milione di computer, prima che Symantec fosse in grado di dire qualcosa. Sì, perché non sono capaci di prevenire un attacco, ma solo di analizzarne uno già in corso, e se il paziente è già morto pazienza, l'importante è poter annunciare l'update. Se la medicina funzionasse come gli antivirus non avremmo i vaccini e saremmo tutti tubercolotici, o qualcosa del genere.

Siamo tutti criminali o c'è qualcuno che fa soldi a spese degli ingenui?

La cosa ancora più divertente è quella frasetta in basso: "Se pensi che questo sito Web sia classificato in modo scorretto, visita l'Internet Security Center di Symantec per farlo presente". E che cosa succederà dopo? Toglieranno il sito dalla lista proibita? Immaginiamoci la coda dei venditori di pornografia all'Internet Security Center. "No, il mio sito non è pieno di schifezze, andate tranquilli!". Se lo tolgono, vuol dire che il meccanismo non funziona (chiunque può chiedere che il suo sito venga escluso dalla lista). Se lo mantengono, vuol dire che il meccanismo non funziona (tutte le stupidaggini contenute nella loro lista resteranno lì dentro per sempre). La deduzione è una sola: il meccanismo non funziona.

Sì, siamo criminali. Colpevoli di scrivere "hacker" nella testata. Gli hacker sono tutto tranne che criminali. Ma per Symantec scrivere hacker è un crimine. Potrebbero provare a scrivere "controllo sprovveduti" invece che "controllo genitori" e vedere se vendono ancora qualcosa.

Nel Far West erano noti i venditori di olio di serpente (snake oil). Imbonitori che andavano di città in città a vendere intrugli di valore zero, a spese dei sempliciotti. Gente come quelli che oggi pensano di proteggere i figli dai pericoli di Internet con i programmi Symantec, invece che con attenzione e affetto.

Theguilty@hackerjournal.it

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE
Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati. redazione@hackerjournal.it

Hanno preso Herr

È un normale ragazzo tedesco di diciotto anni, e non certo un criminale incallito. Ma qualcuno guadagnerà molti soldi da Microsoft

I soldi fanno miracoli. Microsoft ha annunciato una taglia di 250 mila dollari per arrivare a trovare l'autore del worm Sasser e, guarda caso, hanno fatto proprio in fretta. Cinque anni fa gli avrebbero offerto un lavoro come consulente in sicurezza, ma oggi le cose sono cambiate.

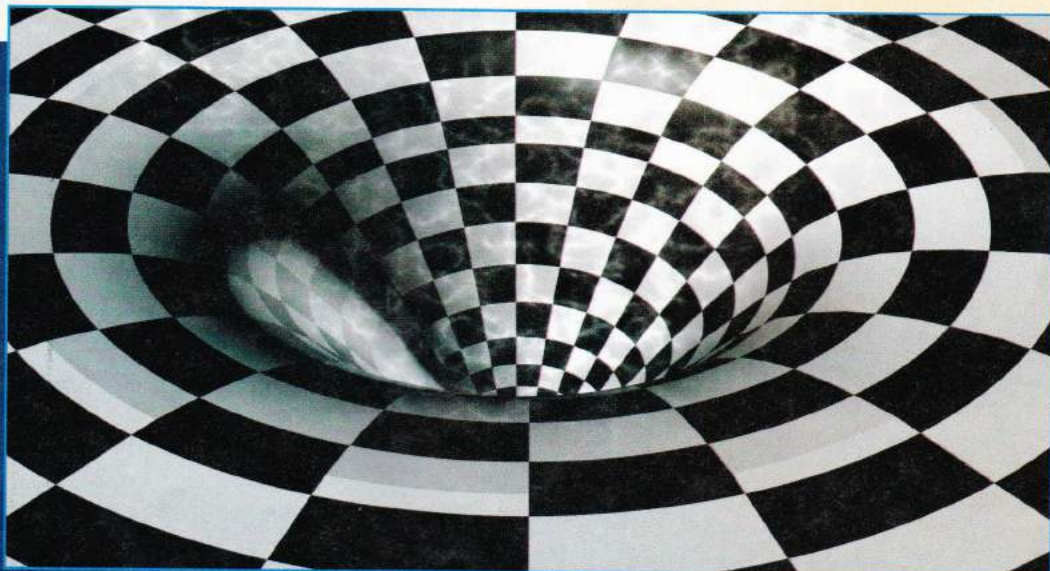
Venerdì 7 maggio hanno arrestato per avere creato e diffuso Sasser un ragazzo tedesco di diciotto anni, studente di liceo, che si dice abbia confessato e sia stato molto collaborativo con le autorità. Ma in realtà deve trattarsi di un gruppo, tant'è vero che subito dopo l'operazione di polizia è uscita comunque una nuova versione di Sasser, che funziona sulla falsariga dell'originale. In ogni caso il ragazzo, di cui si sa solo che vive a Waffensen, vicino Brema, per ora è stato rilasciato, ma rischia un processo e una condanna fino a cinque anni, se verrà giudicato da un tribunale per adulti. Essendo diventato maggiorenne solo il il 29 aprile scorso, tuttavia, potrebbe essere giudicato da un tribunale per minori e cavarsela molto meglio. È stato individuato grazie a cinque suoi conoscenti, ingolositi dal frusciare dei dollari.

Microsoft ha stanziato ben cinque milioni di dollari per un fondo di ricompensa a chi aiuta a trovare i creatori dei virus. Forse sarebbero soldi spesi meglio per migliorare la sicurezza di Windows.

COME FERMARLO

Per distruggere Sasser usiamo il Task Manager di Windows e terminiamo il processo avserve.exe. Poi cancelliamo la chiave di Registry HKLM\Software\Microsoft\Windows\CurrentVersion\Run\avserve.exe. Prima di installare una patch di protezione può essere necessario dover bloccare manualmente la porta 445, perché il worm cerca comunque di impedire la riparazione del sistema. Sono disponibili istruzioni più dettagliate all'indirizzo http://www.microsoft.com /security/incident/sasser.asp.

L'INIZIO DI SASSER

Sasser utilizza l'exploit di buffer overrun MS04-011 LSASS (http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx) rilasciato da houseofdabus il 29 aprile scorso. L'eseguibile è stato compilato il 30 aprile, entro un giorno da quando si è saputo della falla. Altera il Registry di Windows, attiva un miniserver FTP per inviarsi ad altri sistemi, attiva 128 processi di scansione alla ricerca di sistemi vulnerabili e chiama a ripetizione la funzione AbortSystemShutdown per evitare che il PC si possa riavviare. È solo l'inizio della sua attività...

TELEFONI E PAGINE

Ho comprato un cellulare che supporta la nuova tecnologia I-mode. I siti che sono disponibili per la navigazione sono tanti e tutti sono stati aggiornati con linguaggio c-html. In rete ho diversi siti e vorrei aggiornarli per renderli visibili anche con questa nuova tecnologia... Dove posso trovare info sul c-html? Un manuale?

Alfonso

Abbiamo pubblicato un articolo relativo a cHTML sul numero 42 di Hacker Journal. Inoltre puoi trovare tutte le specifiche dello standard allíindirizzo http://www.w3.org/TR/1998/NOTE-compactHTML-19980209/.

◄ ***Un sito fatto come si deve deve essere compatibile anche con il cHTML, il linguaggio di descrizione di pagine Web per cellulari.***

CORSI PER HACKER CERCANSI

Volevo sapere se eravate a conoscenza di qualche corso o simili anche non ufficiale o certificato a Roma o dintorni... Perchè sono convinto che in tutto ciò che gira su Internet o anche per esempio sulla vostra grande rivista non c'è veramente tutto ciò che un hacker deve sapere!

K.M.

Dici che non c'è su Internet, non c'è su Hacker Journal, ma c'è a Roma e dintorni? :-)

▲ ***La strada per diventare hacker. Riquadrato in rosso, il punto esatto in cui si è imparato tutto quello che c'era da imparare.***

Certamente non ci sono corsi di Cose Che Non Girano Su Internet Ma Un Hacker Deve Sapere... altrimenti non ci sarebbero hacker, ma solo saputelli che-hanno-fatto-il-corso.
Battute a parte, l'unico modo per sapere tutto è darsi da fare, e scoprirlo.

LA CHIAVE DELLA POSTA

Sono alla ricerca di un programma (possibilmente gratuito) che mi permetta di scaricare su una "chiave" USB la posta di vari account precedentemente salvati senza modificare le impostazioni e i registri dei computer in cui momentaneamente mi trovo.

Luca

△ ***Ci sta un sacco di posta!***

Non ce n'è bisogno; individua le cartelle in cui il programma di posta che usi conserva i messaggi e copiale sulla chiave come si fa normalmente trasferendo file da un disco all'altro.

I SEGRETI DEL SATELLITE

Ciao, sono un ragazzo di 14 anni che adora il computer.Volevo conoscere il mondo dei satelliti e delle smart card. Come funzionano questi codici Irdeto1, Irdeto2, Seca1, Seca2 e NDS? Perché cambiano ogni giorno i codici e che programma usano x programmare?

Tobie The Saint

La risposta alla terza domanda è: boh, ma non importa. Useranno un qualunque linguaggio di programmazione che gli consenta di raggiungere i risultati che ottengono. La risposta alla prima domanda è: un po' alla volta, se ci segui con pazienza, sveleremo tutto lo svelabile. La risposta alla seconda domanda è: per scoraggiare i pirati, che possono decifrare la codifica in poco tempo, ma non se ne fanno niente se intanto la codifica è cambiata.

UN FLAT PIÙ ESOSO DELLE FLAT

Possiedo un Nokia 9110. Un flat cable, quello che collega la tastiera al display interno del cellulare, si è, con l'uso, leso irreparabilmente e necessita di sostituzione. » impossibile vedere i fax da spedire, il collegamento a internet, spedire messaggi etc. I Nokia point di Milano contattati, c.so Magenta e v. Ricordi (in pratica tutti quelli che ci sono a Milano), hanno dichiarato che la riparazione è possibile e costa ben 170 euro, hanno prezzi fissi, da listino e non importa se devono cambiare un flat cable o il display intero, la cifra è la medesima! Naturalmente è impossibile trovare il flat cable presso rivenditori o riparatori di cellulari, o almeno io

non ci sono riuscito! Morale, o spendo 170 euro per la riparazione e mi ritiro in un monastero per meditare sulle follie del mercato o mi sciolgo il fegato con del buon whisky scozzese e butto il 9110 nella baia di Edimburgo. Ma è possibile che con tutti gli smanettoni al mondo non ci sia qualcuno che sa costruire un fottuto flat cable ad hoc? » così difficile? Almeno voi mi potete aiutare con qualche dritta?

*Alberto un po' disperato
un po' incazzato*

La logica del mercato è spietata, Alberto. Se non avessero queste politiche assassine di riparazione dovrebbero vendere i cellulari a prezzo più alto, ne venderebbero meno eccetera eccetera...
Ci sarà nel mondo uno smanettone disposto a costruire un flat cable per un Nokia 9110? Ci scriva, siamo qui.

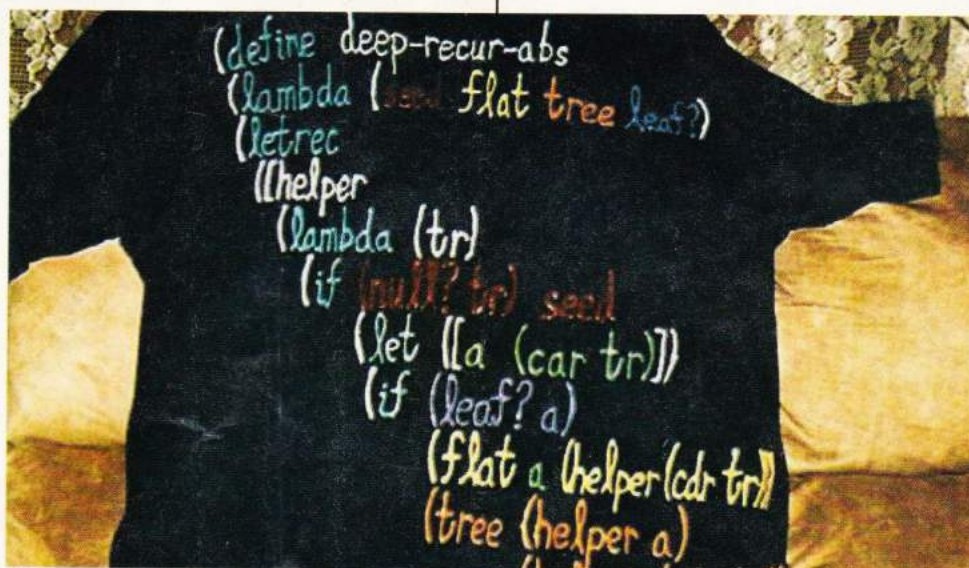
PROGRAMMI A SCADENZA

Vorrei sapere su quale meccanismo si basano i programmi trial che consentono il loro utilizzo per un determinato numero di giorni (30 gg). » possibile che sia sufficiente spostare la data di sistema per aggirare líostacolo?

Enzo

» possibile: dipende dal programma. Quelli stupidi sono ingannabili in questo modo. Quelli meno stupidi hanno meccanismi più sofisticati che si accorgono dellíimbroglio.
Succede un po' la stessa cosa se invece di spostare indietro líorologio di sistema si reinstalla la stessa trial sperando che duri altri trenta giorni. I programmi stupidi non se ne accorgono, ma quelli meno stupidi lasciano traccia della precedente installazione nel sistema, da un semplice file di preferenze fino alla modifica del registro di Windows (o analogo in altri sistemi operativi).

HACKER SI DIVENTA, SEMPRE

Avrei piacere che mi indicaste la strada + breve e semplice x avvicinarmi al mondo del cracking; partite dal fatto che ho bisogno dell'A-B-C di tutto quello che servirà. Io sono bravino a usare Windows, me la cavo con líhardware e di mestiere faccio il disegnatore CAD, ma non ci capisco niente e sottolineo niente di programmazione o simile. Un amico che iniziava ad insegnarmi qualcosa mi ha dato, Softice, un editor esadecimale e altri programmini. Ma che ci faccio? ho letto sulla rivista i libri che consigliate, vanno bene anche x me?

simone

Al mondo del cracking non desideriamo avvicinare nessuno. Se invece vuoi avvicinarti all'hacking, che insegue la conoscenza e non il potere, allora... che cosa ti interessa? Reti, sistemi operativi, motori a scoppio? Non si può sapere tutto. Individua un tuo campo di interesse e comincia da zero, lì. Magari è l'open source. Inizia a giocare con Linux, Darwin, FreeBSD o un altro Unix. Magari è la programmazione. Inizia a giocare con Python o con Perl. Magari è altro... inizia a giocare. Inizierà anche il tuo viaggio verso l'hacking.

Nuova Password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troveremo arretrati, sfondi, informazioni e approfondimenti interessanti. Con alcuni browser, può capitare di dover inserire due volte gli stessi codici. Non fermiamoci al primo tentativo!

USER: passw

PASS: user

HOT!

DECRETO URBANI: È TUTTO PIÙ CARO

Dai commenti non si capisce più nulla. La miscela di rifacimenti, ripensamenti ed emendamenti che doveva trasformare il decreto Urbani in una legge seria, si è fermata di fronte all'approvazione alla Camera di una leggiucola che dice tutto e il contrario di tutto. Rimesse dentro tutte le sanzioni anche per gli utenti privati, che le precedenti promesse davano per cancellate, ora anche i ragazzini sono perseguibili se lo fanno "per fini di lucro". Cosa vuole dire? Perché è stata cambiata la dizione "per trarne profitto", che era l'ultima modifica introdotta in modo da blindare, almeno parzialmente, chi scarica per uso personale?

C'è chi dice che il fine di lucro è più generico del trarre profitto e quindi siamo perseguibili ancora tutti quanti. La questione non è banale, dato che la pena è qualcosa come tre anni di reclusione e 15.000 Euro di multa.

Comunque gli unici a uscirne con le ossa meno rotte sono i provider, che avendo affilato tutte le armi possibili, compresa una denuncia alla Comunità Europea, hanno ottenuto di sfilarsi dal gioco e quindi non saranno più gli sceriffi del web, non avendo alcun obbligo di segnalare comportamenti degli utenti considerati illeciti. Una cosa è comunque ben chiara: il decreto introduce una gabella pari a 0,36 euro per GByte su qualunque supporto di memorizzazione digitale, mentre per i masterizzatori e i software di masterizzazione il sovrapprezzo sarà del 3 per cento sul prezzo di listino. I soldi raccolti dovrebbero andare, passando per la SIAE, agli autori di opere d'ingegno. Ad oggi siamo in attesa dell'approvazione in Senato, dove ancora pochi daranno battaglia. Ma... la Comunità Europea non si è ancora pronunciata, affermando che esaminerà il decreto nei dettagli. La speranza è l'ultima a morire e la Rete, pure.

Il decretone, del peer to peer fa un sol boccone...

LO SCIACQUONE MUSICALE

"Dove sei?" "In bagno!" "Cosa stai facendo?" "Sto ascoltando il nuovo album di Ron!" ed è tutto vero! Comodamente seduti, sciacquati da un apposito getto che compare a comando, asciugati con una brezza calda la cui temperatura è variabile al premere di un pulsante, stiamo godendo del nuovo WC multimediale di Inax (www.inax.co.jp). E' dotato di tutto e ci farà dimenticare perfino la carta igienica, al cui posto mettiamo la "remote control unit", ovvero il telecomando delle funzioni principali. Una dimostrazione? Ma certo! Troviamo il filmato completo all'indirizzo http://www.satis.jp/index2.html. Qualcuno ha già coniato un logo alternativo: Sit Different, e anche qualche immagine che ricorda qualcosa d'altro. Ma, a parte gli scherzi, è tutto reale: un salto tecnologico per andare tutti a ca...

Chi ha detto Sit Different?

WC e MP3: uniti per il nostro relax

I diffusori Hi-Fi all'interno del WC

Al posto della carta igienica e del telecomando stereo: la consolle di controllo

VIRUS HIT-PARADE

Ecco l'elenco dei virus più diffusi, per numero di siti infettati, a tutto aprile 2004:

Posizione per diffusione	Nome con cui è conosciuto	Tipologia	Tendenza alla diffusione	Data inizio
1	W32/Netsky	Worm	+	Febbraio 2004
2	W32/Bagle	Worm	=	Gennaio 2004
3	PE_NIMDA	Worm	Ritorno	Ottobre 2001
4	W32.Welchia.B	Worm	Ritorno	Agosto 2003
5	PE_VALLA	File infector	New entry	Maggio 2003
6	JAVA_BYTEVER	Java applet	New entry	Maggio 2003
7	PE_PARITE	File infector	Ritorno	Gennaio 2004
8	W32/MyDoom	Worm	-	Gennaio 2004
9	W32/Sober	Worm	-	Dicembre 2003
10	W32/Swen	Worm	=	Settembre 2003

GOOGLE? E DOV'È?

Ci siamo mai chiesti dove vanno a finire tutte le nostre ricerche che scriviamo sulla pagina di Google? Ecco, vanno a finire qui, ovvero a Mountain View in California, la sede di Google fotografata da Jeff Carlick.

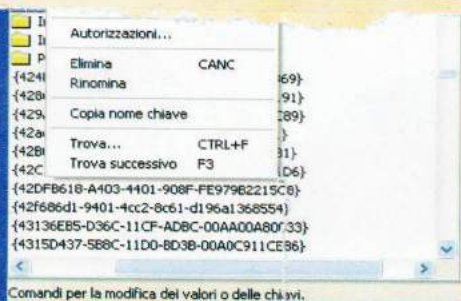
È IN EDICOLA IL SECONDO NUMERO!

Webmaster Journal è la rivista ideale per chi vuole creare un sito internet da zero e metterlo in rete senza fatica in pochissimo tempo. Che si tratti di fare un lavoro su commissione o di creare pagine Web per mostrare la nostra abilità, Webmaster Journal è lo strumento più semplice e immediato, perché tratta tutti i temi caldi di internet, dalla progettazione dei siti alla scelta degli strumenti e dei programmi per realizzare efficacemente i nostri progetti. Ogni pagina fornisce istruzioni che possono essere usate subito apportando delle semplici modifiche alle pagine che vengono incluse sul CD. Inoltre, nel CD di questo numero di Webmaster Journal si trova la versione completa della raccolta di programmi Acdsee 4.0 Powerpack. La raccolta, gratis per i lettori, comprende AcdSee 4.0, Foto Canvas e Foto Angelo: tre strumenti per trattare le immagini impareggiabili per potenza e semplicità d'uso. Sul CD si trovano anche programmi di grande utilità come EZTimeSync 3.7 o Antenna Web Design Studio, e strumenti di livello professionale come Flash MX 2004 e Fireworks MX 2004. Oltre ai consigli e alle guide pratiche che troviamo nelle pagine di Webmaster Journal, possiamo approfittare anche delle raccolte di modelli gratuiti per pagine web e sfruttare i moltissimi elementi già pronti che rendono più facile la vita di chi lavora con Internet. Infine, uno staff di esperti è a disposizione per risolvere i piccoli intoppi che ogni giorno si presentano al webmaster. Webmaster Journal è la rivista per chi vuole fare soldi e divertirsi con il Web.

HOT!

P2P: 477 CITATI IN USA

L'industria discografica americana insiste sulla strada delle citazioni in tribunale di privati che si sono scambiati file MP3.

Undici le università coinvolte, quattrocentosettantasette le segnalazioni di indirizzi IP associati ad altrettanti utilizzatori di sistemi P2P che si sono distinti per quantità di materiale scambiato. Cary Sherman, presidente del gruppo che consorzia i produttori discografici, ha affermato che l'intento è di ricordare alle persone che così commettono un reato e anche di attivare scuole e università perché mettano in atto tutte le misure sufficienti a scoraggiare tali scambi di file. Continuano a remare con i metodi tradizionali, quando ogni giorno su Internet nasce un nuovo metodo di comunicazione e tutto si evolve a rapidità impressionanti. Se tanti sforzi (e tanti soldi) venissero impiegati per trovare vie alternative al commercio discografico, non sarebbe tempo guadagnato?

▲ *Attivato Regedit usiamo la funzione Trova...*

to prendiamo nota, allargando per bene le colonne ObjectName e Location. Catturiamo la schermata o trascriviamo i codici su un foglio di carta: non si sa mai.
Attiviamo Start -> Esegui -> Regedit e con Ctrl+F attiviamo la funzione Trova. Inseriamo nella casella di ricerca la stringa del codice indicato sotto ObjectName e individuiamo l'infezione. Controlliamo bene che sia giusto il codice e

Risorse del computer\HKEY_CLASSES_ROOT\CLSID\{4224AC84-9B11-35

▲ *Individuato con certezza l'oggetto spione, un clic destro e lo eliminiamo all'istante.*

HACKER

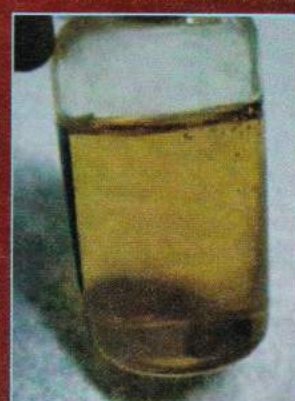
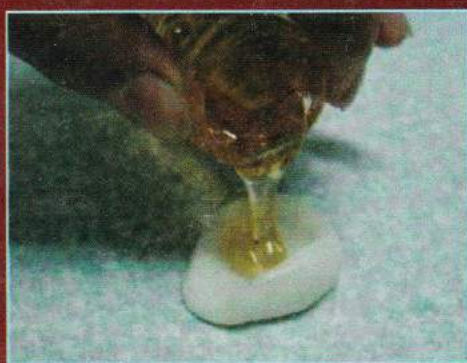
atina

ai più efficiente
er farlo servono:

iquida)

Installiamo e avviamo

L'installazione richiede minuti. Un clic e siamo tro. Un altro clic su Scan e attiviamo la ric di spyware e altre si

a. Scaldiamo la morbidirla e presito su essa per plastica, raffred-

Versare la miscela di acqua e gelatina nello stampo e mettere a raffreddare in frigo

La gelatina andrà prevedibilmente versata nello stampo, che metteremo in frigo per una decina di minuti almeno, il tempo necessario perché la gelatina si rapprenda. Il dito è pronto! Il dito così ottenuto è molto simile al dito originale, costa molto meno di un dito al silicone e funziona egregiamente anche con i sensori capacitivi, che non si lasciano ingannare dal dito al silicone. Tutta la procedura è effettuabile da qualsiasi ragazzino abbastanza sveglio da essersi procurato plastica e gelatina. Ma non è tanto importante che sembrino uguali all'occhio. Occorre che a essere ingannato sia il sensore. Ebbene, un sensore ottico cattura immagini tutto sommato simili di dita al naturale, al silicone o alla gelatina. La cosa interessante è che un sensore capacitivo rifiuta un dito al silicone, ma dà via libera a quello in gelatina.

▲ Al naturale (sinistra), al silicone (in mezzo) e alla gelatina: ecco come il sensore ottico vede tre impronte digitali, di cui due fabbricate artificialmente.

Certo, dirà qualcuno, tutto molto interessante, ma resta il fatto che bisogna avere il dito originale per farne una copia, e questo dà una certa sicurezza. Ovvio, ma aspettiamo il prossimo articolo, quello in cui spiegheremo come si ricava un dito artificiale da un'impronta lasciata in giro...

Barg the Gnoll
gnoll@hackerjournal.it

▲ Da sinistra a destra: carne e ossa, silicone, gelatina. Il risultato si commenta da solo.

▲ Ecco come il sensore capacitivo vede il dito vero (a sinistra) e il dito di gelatina.

COLPEVOLE? GNAM, GNAM

La tecnica del dito di gelatina è stata provata da vari collaudatori su almeno undici lettori diversi di impronte digitali, superando l'80 percento di efficacia nell'ingannarli.
Nei casi in cui veniva misurata anche l'umidità del dito è bastato bagnare quello finto; nel caso inoltre di una sorpresa imprevista da parte delle forze dell'ordine, basterebbe... mangiarsi il corpo del reato!

GUERRA AI LADRI DI AUTO

I moderni antifurti sono sofisticatissimi e utilizzano tecnologie di crittografia avanzate. Vediamo quali.

Si chiamano immobilizzatori e sono composti da due componenti principali. Il nocciolo del sistema è il transponder, ovvero la chiave dell'automobile, che funziona assorbendo l'energia che gli serve senza bisogno delle pile. Nella nostra automobile è infatti montato un transceiver che genera un campo magnetico ad alta frequenza che è irradiato da un avvolgimento che fa da antenna. L'energia inviata alla nostra chiave sotto forma di onde elettromagnetiche è sufficiente per alimentarla e attivarla, così che si mette a funzionare e decodifica i dati che arrivano dal transceiver sotto forma di segnali radio.

Segretezza e crittografia

Il riconoscimento del fatto che siamo noi i veri proprietari dell'auto può avvenire in molti modi, per esempio chiedendoci un codice, oppure tramite il riconoscimento della nostra impronta digitale. Ma nessuno di questi sistemi potrà mai essere tanto comodo quanto quello che viene ormai adottato da quasi tutti: la proprietà. Il fatto stesso di possedere la chiave per entrare in auto e accendere il motore è il sistema più comodo, più conosciuto e più sicuro anche in casi di emergenza. Per rendere sicuro questo metodo dobbiamo però fare in modo che la chiave si comporti come un transponder e che il codice inviato dal trasmettitore corrisponda a quello memorizzato nella chiave stessa. Rimane però un problema, a pensarci bene. L'autenticazione è a senso unico: l'auto riconosce la chiave, ma non viceversa. Per rendere più sicuro il tutto, allora, siamo costretti a usare il sistema che viene chiamato mutua autenticazione, dove tutti e due i sistemi si riconoscono tra loro. Un sistema di questo tipo è quello a domanda e risposta, quando l'automobile invia una richiesta alla chiave (la domanda) e quindi verifica che sia giusta la risposta che riceve dalla chiave. Tra l'altro la domanda e la risposta possono variare a ogni ciclo e, durante l'uso dell'auto, tra i due non viene scambiato nessun messaggio, mantenendo così la segretezza.

UNITA' DI CONTROLLO — TRANSCEIVER — ANTENNA — TRANSPONDER

▲ *Niente pile dentro la chiave: l'energia è assorbita via radio*

CENTRALINA ANTIFURTO — domanda di 40 bit casuali — CHIAVE DELL'AUTOMOBILE

Random # Generator, Encryption Key, Software Encryption Routine, Transceiver, Signature, Signature, Compare, Immobilizer Controller, Accensione/No accensione, firma di risposta a 24 bit, RF Interface Circuit, Challenge Register, Encryption Circuitry, Encryption Key, Response Register

▲ *A domanda rispondo, e sempre in modo diverso!*

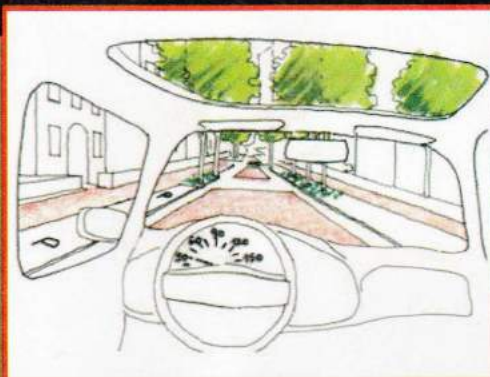
Segreto assoluto

I cripto transponder funzionano proprio sul principio della domanda e della risposta. Durante la fase di inizializzazione del colloquio tra

ALIMENTAZIONE MAGICA

Per l'alimentazione senza pile si usano due sistemi.

SISTEMA FULL DUPLEX

L'energia generata dall'antenna della centralina e i dati che devono essere trasmessi viaggiano contemporaneamente, in un unico momento.

SISTEMA HALF DUPLEX

Prima viene trasmessa dall'antenna l'energia sufficiente a caricare un condensatore all'interno della chiave. Quando la chiave è così alimentata e pronta per funzionare, ovvero qualche millisecondo dopo, l'energia accumulata viene usata per decrittare i dati in arrivo e per dare la risposta alla centralina.

transponder e centralina si scambiano la chiave segreta crittata. La chiave non può essere letta: viene letta solamente la risposta alla domanda inviata dalla centralina. Normalmente la centralina antifurto genera una domanda fatta di 40 bit generati a caso e la invia alla chiave dell'auto tramite la codifica PWM (modulazione ad ampiezza di impulsi). Nella chiave dell'auto la sequenza viene memorizzata e viene generata una sequenza di risposta lunga 24 bit. Il tutto nel periodo di tempo in cui c'è sufficiente energia per funzionare…
La risposta viene inviata alla centralina tramite la modulazione a spostamento di frequenza (FSK). La centralina calcola al suo interno la risposta che si aspetta e la confronta con la risposta ricevuta: se coincidono, il motore della nostra automobile si accende.

I vantaggi di questo sistema? Sono ovvi:
- la risposta è sempre diversa e dipende dalla domanda, quindi è una autenticazione dinamica;
- dopo le fasi di inizializzazione del colloquio tra centralina e chiave dell'auto, non è inviato nessun dato critico intercettabile;
- la chiave crittografica non può essere letta dall'esterno;
- la chiave dell'auto non può essere duplicata;
- se lo desideriamo la stringa per criptare i dati può essere bloccata in modo irreversibile o alterata per diventare inutilizzabile.

Scardinamento

Ovviamente tutto quello che crittato è, in teoria, decrittabile dopo un certo numero di tentativi. Ma in applicazioni come la chiave di un automobile possiamo considerarci al sicuro se
- l'attaccante deve spendere più di cin-

GIÙ LE MANI DALLA MIA MACCHINA!

que minuti per provare;
- la chiave varia comunque il codice entro dieci giorni
- l'attaccante non è così esperto di tecniche di criptoanalisi.

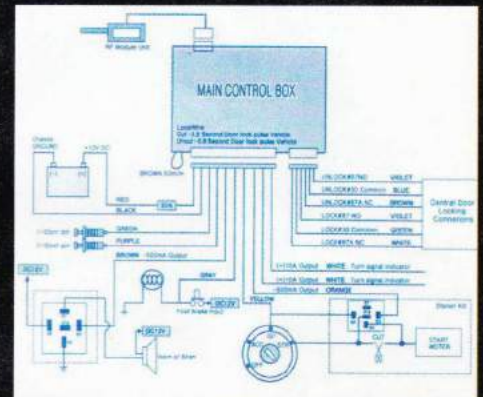
Quanto tempo ci impiegherebbe un ladro esperto a decifrare la stringa crittata con una tecnica, per esempio, di scanning?

Supposto che il ladro si metta a trasmettere una risposta causale a ogni domanda generata dalla centralina, il tempo medio per azzeccare la risposta giusta è dato dalla formuletta:

$$t = R * 2 ^ (rb-1)$$

in cui rb è la lunghezza della risposta in bit e R è il tempo di ripetizione della centralina in secondi. Supponiamo che questo tempo sia di 200 millisecondi. La risposta sappiamo che è lunga 24 bit. Il tempo medio per azzeccarla giusta diventa di 19,4 giorni. Probabilmente non lasciamo completamente incustodita l'automobile per così tanto tempo. Se lo facciamo, mettiamo nel box brandine, panini e birre: anche il ladri hanno bisogno di interrompere, ogni tanto, per mangiare...

In realtà la circuiteria interna alla centralina è in grado anche di inviare una serie di messaggi di controllo che individuano se ci sono anomalie nel cir-

cuito della chiave, se la chiave non riesce ad assorbire l'energia sufficiente per autoalimentarsi e così via. Ma qui siamo già nel campo della microcircuiteria elettronica, che ormai fa uso di chip dedicati sia nella centralina che all'interno della nostra chiave.

Un ultimo avvertimento? Non perdetela!

ControlBus
standardbus@softhome.net

Distrazione Fatale

Era come un rally. Lui e CrazyFinn, due squadre opposte con un unico scopo: VINCERE

Alle quattro e sedici minuti Widget si svegliò di soprassalto con un unico pensiero: penetrare nel server della sua società; anzi della sua ex-società, dato che appena prima dell'uscita dal laboratorio era stato chiamato dal suo capo e in tre minuti secchi anche licenziato.
L'indomani si sarebbe attaccato al telefono, avrebbe chiamato l'avvocato del lavoro, sentito il parere dei sindacati, pianto di rabbia e poi smaltito tutto con una partita sulla XBox a "Dead or Alive Xtreme Beach Volleyball", e con una Slalom Lager appena stappata: un bel nove percento d'alcol di malto.

Intanto, però, voleva dargli una lezione. Che si ricordassero per sempre di Widget. Anche se non lo conoscevano sotto quel nick.
L'aveva scelto tra quelli delle squadre di rally, la sua passione. Una passione che condivideva con CrazyFinn, il suo collega responsabile della sicurezza informatica. Era il suo nick dei momenti di battaglia, delle sfide ai sistemi di mezzo mondo fatte al riparo dell'anonimato.

Apparve sul suo Treo600, l'immagine di Flora

Il nome di dominio lo conosceva bene e altrettanto bene sapeva del firewall che, tra l'altro, era stato installato solo di recente. Inutile cercare di penetrare da lì.
Ma un tentativo lo fece lo stesso, quasi per scaramanzia. L'intenzione era lucidamente presente nella sua testa: trovare tutti i domini collegati appartenenti alla sua stessa ex-azienda, e vedere se almeno uno era per caso fuori dal controllo del firewall.
Si attaccò a un wohis che gli aveva dato sempre buone soddisfazioni e come immaginava otto IP erano esattamente legati a una registrazione fatta proprio dal suo capo.
Gli scappò un sorriso, ma sapeva che era ben poca cosa. Probabilmente non avrebbe mai superato il firewall. Sapendo a cosa stava per andare incontro, decise di attivare ogni difesa in suo possesso. Aveva una scorta di quattro sistemi in cui poteva penetrare da back-door appositamente lasciate aperte, in tre società differenti. Un bottino acquisito negli ultimi sei mesi, di cui andare orgogliosi con nessuno: il suo segreto.

Usò telnet dall'uno all'altro e per ulteriore sicurezza installò sul terzo di questi sistemi un root kit che aveva trovato in rete e che impediva al sistema ospite di loggare in qualunque modo qualunque le attività. Prima che potessero beccarlo, avrebbero passato settimane a cercare in un posto sbagliato e, per di più, non trovando traccia di movimenti sospetti. Al massimo individuando il trojan utilizzato: ma ormai era fatta.

Dal terzo server alternò l'uso di uno scanner e di Strobe verso la sua società, sperando di trovare una porta in ascolto. Ma non ne ebbe il tempo.
A casa di CrazyFinn, dopo un breve e melodico squillo, apparve sullo schermo del suo Treo600 l'immagine di Flora, la sua assistente dell'ultimo turno della notte, che gli segnalava un evidente e massiccio tentativo di intrusione. CrazyFinn era l'amministratore del complesso sistema di server posizionato in quello che gli altri chiamavano "il bunker di Crazy". Era abituato alle decisioni improvvise, da secondo pilota. Il suo istruttore, all'autodromo, gli diceva sempre di non distrarsi, di concentrarsi. Un attimo di troppo e la gara era persa. Un attimo di meno e la vittoria era in mano. Ci mise solo tre secondi, a decidere: non poteva fare altro che chiudere tutte le porte momentanea-

mente, e così fece. Flora eseguì: off. Il mattino dopo, dall'analisi dei log, trovò l'attaccante: una società di gomme da masticare. Una telefonata al suo webmaster sarebbe stata sufficiente per avere la conferma che cercava: impossibile risalire al mittente dello scherzo. Doveva essere un vero bastardo, un esperto bastardo.

Widget se ne accorse subito, ma non poteva fare granché. Capiva di essere arrivato a un punto morto e decise per un'altra strategia. Immaginò Flora e CrazyFinn alle prese con un'intrusione da un'innocua società e le loro facce. Ci prese gusto, quasi si sarebbe divertito e gli avrebbe telefonato, in altre circostanze. Ma adesso voleva che soffrissero e poteva farlo, anche se non subito.

GERGO E SOFTWARE

Tutto sui trojan root kit: http://www.security-labs.org/index.php3?page=404

Dove trovare Strobe:
ftp://ftp.scn.ru/pub/soft/unix/distfiles/strobe-1.06.tgz
Strobe è uno strumento che individua e descrive tutte le porte tcp in ascolto su un host remoto o su molti host differenti ottimizzando il consumo di banda e l'occupazione del sistema individuato.

WAR-DIALLER:
chiama un elenco di numeri telefonici fino a individuare la risposta di un modem. Un esempio è Shokdial che si trova presso: **http://www.w00w00.org/files/misc/shokdial/shokdial.c**

La notte seguente

Non era nemmeno andato a letto. Era stata una giornataccia, piena di telefonate agli uffici di una mezza dozzina di legali amici e di amici di legali. Una caraffa appena appoggiata a una pila di manuali lo teneva adrenalinico alimentandolo di caffé scuro. Rammentò di avere, da qualche parte, un war-dialler che sapeva fare egregiamente il suo lavoro: ShokDial. Sapeva bene che, come in qualunque grande società, c'è sempre qualcuno che attacca al PC un modem esterno, per fare i suoi comodi. Per chiamare da casa senza avere accesso alla rete aziendale, per esempio. Sapeva che tra le centinaia di suoi ex colleghi ci sarebbe stato sicuramente il furbo che aveva trasgredito alle regole del "bunker".
E sapeva anche da quale numero iniziavano e a quale numero finivano tutti gli interni. Programmò la scansione di ShokDial e ci mise circa un'ora e mezza.
Ma alla fine il confortante tono della portante di un modem era in linea. Prese nota e richiamò. Aveva deciso per un attacco brute force, non appena a video gli fosse apparsa una qualche schermata di richiesta UserID e password. E così fece. Se era come sul suo ex PC, "nome dot cognome" servivano per bollare tutto: dalla posta elettronica al tesserino di riconoscimento, passando per lo UserID, appunto. La password fu un gioco da ragazzi. Col primo attacco fece bingo in meno di sette minuti: password uguale a "ugo". L'ingenuo. Era dentro. Da una porta laterale, certo. Ma era dentro. Provò a installare un keylogger e ci riuscì ("bene" si disse "mi ci voleva un administrator scemo!"). Poi andò a dormire. Non c'era da fare niente altro che aspettare qualche giorno.

Il rally lo vince uno solo

Passarono tre settimane, ma alla fine qualcuno del "bunker", come Widget dedusse dal file del keylogger, s'attaccò al PC e fece un sacco di manutenzione. Aprendo e chiudendo diverse volte un collegamento al server Web. Con password e ID, naturalmente. Tutte accuratamente riportate dal bravo keylogger. Fu un attimo. La home page tanto amata dal suo boss venne sostituita sul server da un'immagine di ragazza, che null'altro aveva addosso se non il boss in persona. Un fotomontaggio a cui aveva lavorato piuttosto grossolanamente, ma faceva il suo effetto. CrazyFinn non si diede pace. Dai log di sistema non risultava nessuna falla del firewall e di un dipendente troppo intraprendente non se ne parlava. Si confrontò con Flora parecchie volte, e con il boss. Decisero di telefonare comunque all'ispettore Wardy dell'FBI, che recentemente aveva trasmesso un'informativa, chiedendo di segnalare ogni possibile attacco, pur piccolo. Robe necessarie a captare in anticipo imminenti atti terroristici verso la rete nazionale, o cose così, gli pareva di ricordare. Poi, nel dormiveglia di una mattina più primaverile di altre, l'illuminazione: serendipity, o qualcosa di analogo. Ecco la soluzione: qualcuno aveva attaccato al PC del suo ufficio un modem non autorizzato. La mattina avrebbe fatto una bella scarpinata, tra ascensori e piani di quella specie di grattacielo a vetri che era la sua azienda.

Basta un attimo

Da lì a risalire a chi aveva chiamato il numero del modem nell'ultimo mese fu questione di qualche tabulato dell'azienda telefonica passato nelle mani giuste. Quando CrazyFinn scoprì il keylogger, l'FBI era già stata a casa di Widget.

◄ *Smaltì tutto con una partita a Dead or Alive Xtreme Beach Volleyball.*

A WEBBIT non

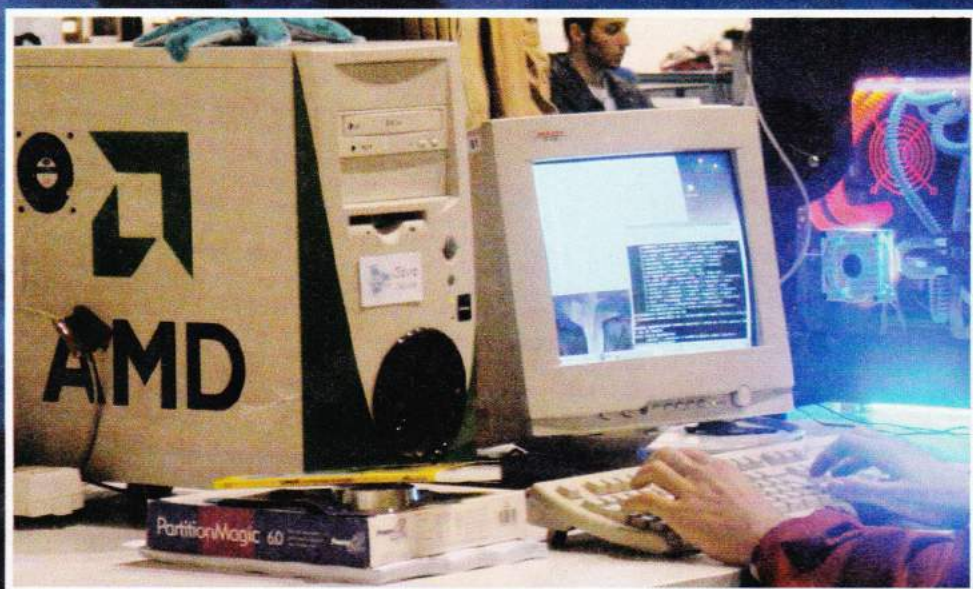
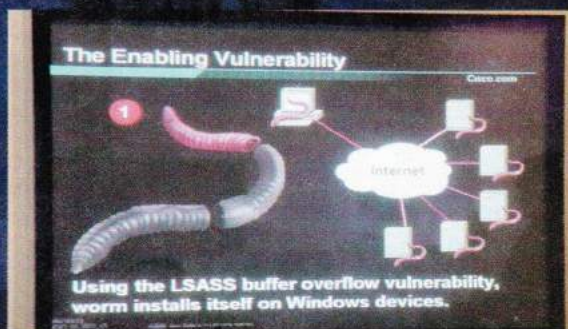
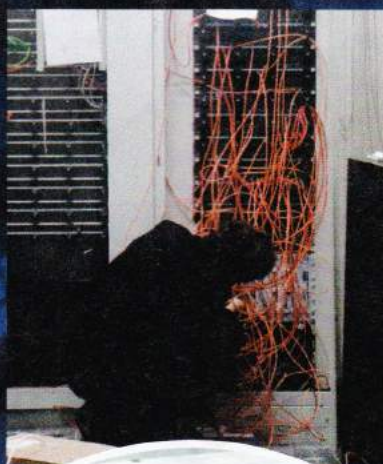
Foto e commenti da Padova, dove si

Scrivo che è appena finito Webbit 2004 (http://webb.it). Tre giorni di manifestazione che per metà è fiera tradizionale, con gli stand, le standiste (!), i biglietti da visita e le brochure. Per metà, invece, è un happening cui partecipano le teste migliori in Italia tra programmatori, hacker, demoer e chi più ne ha più ne metta. Partecipano community i ogni genere, da sikurezza.org a più Java User Group di quanti se ne possano contare, fino ai grup-

pi che si occupano di software specifico come Debian, Zope, OpenBSD, Perl e qualsiasi altra cosa possa venire in mente…

…Le community hanno la possibilità di tenere seminari in cui presentano il proprio lavoro e le proprie conoscenze, affollati di pubblico di ogni genere. E hanno uno spazio proprio per distribuire volantini, vendere t-shirt o altri gadget per autofinanziarsi, o semplicemente per conoscere gente nuova…

si dorme MAI

radunano le crew più toste del momento!

...Il bello arriva quando cala la sera. La parte business sparisce e l'arena rimane aperta tutta la notte, 24 ore su 24. Nella notte si svolge di tutto: Nutella party, proiezione abusiva di film (quest'anno Kill Bill 2, per esempio, ma anche i Simpson), gare di frisbee negli spazi aperti tra uno stand e l'altro, guerra dei woofer tra chi si è portato dietro non solo il computer ma anche le casse (sì, ognuno si porta il computer da casa, e nessuno si azzarda a rubare uno spillo), code marathon in cui un pugno di programmatori inizia a scrivere codice e va avanti fino all'alba eccetera eccetera. Una notte è passato anche Dj Spiller con il suo Mac!...

...C'erano server di prova messi lì apposta per esercitarsi a diventare veri hacker, sfide tra robot programmabili, esibizioni di realtà virtuale, antenne wireless da tre chilometri realizzate con vecchie latte d'olio e molto altro. Lasciamo la parola alle foto, che raccontano meglio delle parole!

Michele Campovecchio
michele_c@hackerjournal.it

Verifichiamo

Qualcuno che conosciamo ha un sito di vendita on-line? Spieghiamogli come si calcola il numero delle carte di credito e come possiamo vedere se una carta può esistere realmente oppure stanno tentando di imbrogliarlo

▲ *Verificare l'esattezza del numero di un numero di carta di credito è questione di pochi istanti.*

Il sistema di elaborazione del numero delle carte di credito può sembrare misterioso, ma in realtà è piuttosto semplice ed è questione di pochi attimi capire se un numero è attendibile o meno. Anzi, l'algoritmo utilizzato è pubblico e pienamente documentato. Si chiama algoritmo di Luhn e serve soprattutto a evitare errori di trascrizione. Non è un vero e proprio sistema di sicurezza, perché come stiamo per vedere è debolissimo.

Come verificare se una carta di credito è reale

Prendiamo il numero di carta che ci interessa, per esempio 4539 9243 3876 3207. Consideriamo le cifre dispari: la prima, la terza, la quinta e così via. Raddoppiamo ogni cifra e, se il risultato è maggiore di nove, sottraiamo nove.

PRENDIAMO LE CIFRE DISPARI:

4 3 9 4 3 7 3 0

RADDOPPIAMO OGNI CIFRA E TOGLIAMO 9 DAI RADDOPPI CHE DANNO COME RISULTATO PIÙ DI 9:

8 6 9 8 6 5 6 0

(I RADDOPPI CON SUCCESSIVA SOTTRAZIONE DI 9 SONO AVVENUTI SULLA QUINTA CIFRA E SULL'UNDICESIMA:

9 * 2 = 18 - 9 = 9 e 7 * 2 = 14 - 9 = 5)

SOMMIAMO I NUMERI OTTENUTI:

8 + 6 + 9 + 8 + 6 + 5 + 6 + 0 = 48

▲ *Questa carta ha un numero pari di cifre e quindi le cifre da raddoppiare sono quelle dispari.*

CALCOLIAMOLO IN C

Questo semplice programma in linguaggio C svolge lo stesso lavoro del foglio di calcolo.

Funziona inserendo le cifre della carta di credito tranne l'ultima, e restituisce l'ultima cifra.

```
#include        <stdio.h>

/*
* Codice di controllo di un nume-
ro di carta di credito
* Digitare le cifre della carta
tranne l'ultima
*/
int codice (v)
char *v;
{
register i, s = 0;
int l, t;

l = strlen(v);
for(i = 0; i < l ; i++)
  {
  t = (v[l - i - 1] - '0') * (1 + ((i + 1)
% 2));
  s += t < 10 ? t : t - 9;
  }
return 10 - s % 10;
}


void main (argc, argv)
int  argc;
char **argv;
{
while (—argc)
   printf ("%d\n", codice
(*++argv));
}
```

le carte di credito

NUMERI DA CONOSCERE

Ecco come sono fatte le carte di credito più diffuse:

Carta	Prefisso	Lunghezza	Algoritmo di controllo
Mastercard	da 51 a 55	16	mod 10
Visa	4	13 oppure 16	mod 10
American Express	34 oppure 37	15	mod 10
Diners Club e Carte Blanche	da 300 a 305, 36 oppure 38	15	mod 10
Discover	6011	16	mod 10
enRoute	2014 oppure 2149	15	vari
JCB	3 (anche 2131 oppure 1800)	16 (15)	mod 10

ORA CONSIDERIAMO LE CIFRE PARI (LA SECONDA, LA QUARTA, LA SESTA...):

5 9 2 3 8 6 2 7

LE SOMMIAMO COSÌ COME SONO, SENZA RADDOPPI:

5 + 9 + 2 + 3 + 8 + 6 + 2 + 7 = 42

SOMMIAMO I DUE TOTALI:

48 + 42 = 90

Il totale deve essere divisibile per 10 senza resti. In questo caso 90 è esattamente divisibile per 10 e quindi 4539 9243 3876 3207 potrebbe essere il numero di una carta di credito autentica. In modo ancora più facile: se la somma finale finisce per zero, il numero è ok.

Se la carta di credito è composta da un numero dispari di cifre, il procedimento è identico, tranne per il fatto che vanno raddoppiate le cifre pari e non quelle dispari.

Il carattere di controllo

L'ultima cifra del numero delle carte di credito è il carattere di controllo. Serve a verificare che le altre cifre siano a posto. Esistono programmini molto semplici che, date le cifre di una carta tranne l'ultima, calcolano l'ultimo numero. A quel punto si può facilmente confrontare il numero ottenuto con quello da controllare per vedere se corrispondono (numero plausibile) oppure se divergono (numero impossibile).

Kurt Gödel
kurtgoedel@hackerjournal.it

IL CREATORE DEL CODICE

Dobbiamo l'attuale algoritmo di generazione e verifica dei numeri di carte di credito a Hans Peter Luhn. Nato il primo luglio 1896 a Barmen in Germania e morto proprio quarant'anni fa, nel 1964, dopo avere totalizzato oltre ottanta brevetti, 67 dei quali ottenuti lavorando per IBM, ed essere stato definito il padre dell'information retrieval. Si può leggere una biografia completa di Luhn all'indirizzo http://web.utk.edu/~jgantt/hanspeterluhn.html.

Un padre dell'informatica e le sue schede perforate (chi se le ricorda?)

ADDIO

Chissà che cosa abbiamo scaricato da Internet, o chissà che cosa c'era dentro quello che abbiamo scaricato!

MA ORA L'IMPORTANTE È LIBERARSENE IN MODO INDOLORE

Chiamiamoli programmi spazzatura, anche se si infilano nella cartella di avvio di Windows, perché il loro vero posto sta nel cestino e perché puzzano. Puzzano di virus, di violazione della privacy, di ingombro inutile del disco e via dicendo. Liberiamocene. Tipicamente i programmi spazzatura si avviano automaticamente perché posizionano un collegamento a se stessi nella cartella di avvio di Windows, di solito c:\Windows\Start Menu\Programs\StartUp. La prima azione da compiere è, quindi, cancelliamo il collegamento al programma spazzatura nella cartella di avvio.

UN VERO FINTO ESEGUIBILE

Si può reperire, per esempio, all'indirizzo http://www.cexx.org/dummy.zip. Il finto eseguibile va messo al posto del programma spazzatura originale, non del collegamento che si trova nella cartella di avvio del computer.

▲ *Che parta Windows è normale. Che parta anche altro insieme a lui, dipende.*

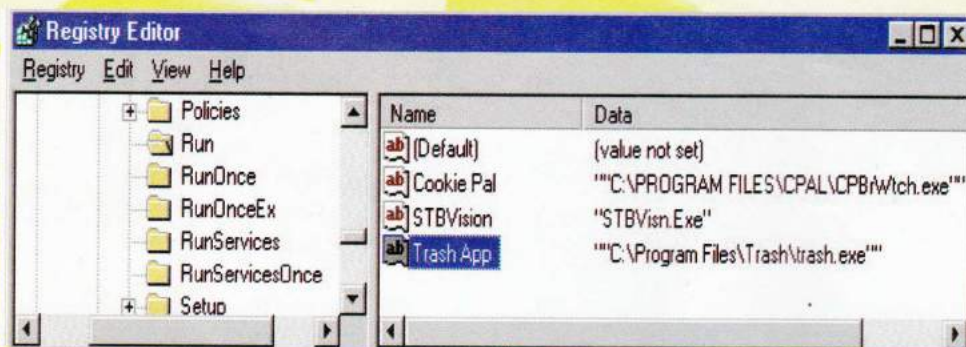
Alcuni programmi, tuttavia, sono più furbi, e sanno reinstallare il collegamento automaticamente se noi lo abbiamo cancellato. La soluzione in questo caso è installare un finto eseguibile. Lo si mette al posto del programma spazzatura (non del collegamento nella cartella Avvio). Il collegamento "lancerà" il nostro finto eseguibile pensando che sia il vero programma spazzatura, non succederà niente e vivremo felici. A scanso di equivoci, conviene dare al finto eseguibile privilegi di sola lettura. Così non potrà essere modificato in alcun modo. Il secondo comandamento è di conseguenza installiamo un finto eseguibile al posto del programma spazzatura.

CENSURIAMO IL CENSORWARE

Per censorware si intende quel software che, ansioso di preservare la moralità della nostra macchina, finisce per mandarla a interfacce di facili costumi. Sono quei programmi come Cyber Patrol, che pretendono di bloccare l'accesso ai siti proibiti da parte dei bimbi (come se loro non fossero ben più abili), oppure gli antivirus impostati in modo così paranoico che la macchina diventa inutilizzabile. Dedicheremo al tema un articolo apposta.

Alcuni programmi spazzatura non infestano la cartella di avvio ma sporcano il file win.ini con riferimenti a se stessi. Lo fanno tipicamente i programmi tipo censorware e la riga contiene una istruzione quale load= o run=, simile a questa:

```
load="C:\Trash\App\programma-spazzatura.exe"
```

PROGRAMMI SPAZZATURA!

Togliamoci di torno anche questo problema. Apriamo il file win.ini in un editor qualunque (va bene anche il Blocco Note!) e cancelliamo la riga in questione dentro il file. Win.ini dovrebbe trovarsi dentro C:\Windows\win.ini. In sostanza: eliminiamo i riferimenti ai programmi spazzatura dal file win.ini.

Il programma non sta né nella cartella di avvio né in win.ini? Il bastardone potrebbe avere installato un riferimento a se stesso nel Registro di Windows. Per toglierlo di mezzo occorre aprire il Registro, con una utility apposita oppure con il comando di sistema Regedit (menu Start -> Esegui -> regedit).

NOTA SUL REGISTRO

Attenzione a operare sul Registro. Commettere una sciocchezza senza sapere che cosa si stia facendo può portare a dover reinstallare Windows.

```
[FontSubstitutes]
Arial Cyr,204=Arial,204
Arial Cyr,0=Arial,204
Arial CE,238=Arial,238
Courier New Cyr,204=Courier New,204
Courier New Cyr,0=Courier New,204
Courier,0=Courier New,204
Courier New CE,238=Courier New,238
Times New Roman Cyr,204=Times New Roman,204
Times New Roman Cyr,0=Times New Roman,204
Times New Roman CE,238=Times New Roman,238
```

▲ *Il file win.ini non è particolarmente fotogenico. Ma un Blocco Note in cirillico non lo si vede spesso!*

In questo caso, nel Registro di Windows, nella cartella Run, troviamo il programma spazzatura TrashApp assieme ad altri, legittimi, che partono insieme a Windows

Quando si apre l'editor di Registro, premiamo F3 per effettuare una ricerca e, nel riquadro che appare, digitiamo RunServices. Nella sezione di sinistra verrà evidenziata una cartella con questo nome, contenente altre cartelle con nomi simili come Run, RunOnce e altre. Clicchiamo su Run: la sezione a destra elencherà i programmi che partono all'avvio del sistema. Sotto Name appariranno i nomi dei programmi e sotto Data il percorso e il nome del file. Cerchiamo il programma spazzatura e distruggiamolo con il menu edit -> delete.

Si dovrebbe vedere il programma spazzatura. A quel punto potremo eliminarlo. Se non è lì, guardiamo nelle altre cartelle "RunQualcosa" e dovrebbe saltare fuori. Se ancora non si fa vedere, premiamo ancora F3 ed esaminiamo la prossima cartella RunServices. Nei sistemi con più utenti le cartelle di questo tipo possono essere numerose.

Michele Campovecchio
michele_c@hackerjournal.it

ESEMPI DA NON IMITARE

Qualche programma che ci ritroveremo a voler togliere da quelli ad avvio automatico:

- **AOL Instant Messenger**: si prende con l'installazione di Netscape Navigator. Mostra in continuazione pubblicità di America On Line (del cui servizio a noi non ce ne può importare di meno) e di altri servizi.
- **RealPlayer**: mostra una serie di "canali" audio e video che in realtà sono solo pubblicità. In più installa una icona di RealPlayer nella barra dei task e occupa memoria inutilmente.
- **QuickTime**: in realtà non dà problemi, ma perché deve caricarsi all'avvio se non abbiamo video o musica da eseguire?
- **Il vecchio TSADBOT** e gli altri programmi il cui scopo è unicamente propinarci pubblicità indesiderata. Quasi un virus. Anche di questi parleremo più a fondo presto!

▲ *Quando troppi programmi vogliono partire tutti insieme occorre che qualcuno dia una regolata.*

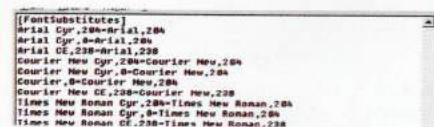



FOTO 3D come

Guardare le foto tridimensionali di Marte fa davvero impressione. Ma non c'è bisogno di andare così lontano per avere lo stesso effetto con le nostre!

▲ L'immagine di sinistra viene convertita in scala di grigio ed entrambe le immagini sono in modalità RGB. Qui si vede Photoshop, ma va bene qualsiasi programma grafico serio. Foto NASA/JPL.

Spirit e Opportunity, i rover della NASA che esplorano la superficie di Marte, hanno speciali fotocamere stereoscopiche con cui scattano immagini da mozzare il fiato, visibili a http://marsrovers.jpl.nasa.gov/home/index.html. Ma possiamo fare lo stesso anche noi, con qualsiasi programma di fotoritocco. L'importante è scattare due foto per soggetto, vediamo come.

VIVA IL BIANCO E NERO

Alla NASA producono anche immagini tridimensionali a colori, ma richiedono occhiali speciali e sono prodotte con tecnologie di polarizzazione e visione su schermi appositi che sono fuori dalla nostra portata. Ma sono affascinanti anche le immagini in bianco e nero.

▲ Si selezionano solo il canali verde e blu.

Persone e angoli

Le persone sono un buon soggetto per le foto 3D, perché tendono a "saltare fuori". Vanno inquadrate con uno sfondo contenente angoli e profondità (sì davanti a una strada, no davanti a un muro). Scattiamo a una distanza di tre-quattro metri e scattiamo due foto: la prima come vogliamo e a seconda spostando l'obiettivo verso destra di circa otto centimetri (più o meno la distanza tra i nostri occhi).
È importante che l'obiettivo rimanga alla stessa altezza dal suolo e si sposti sono in orizzontale, restando alla stessa distanza dai soggetti .
Questi ultimi, tra una foto e l'altra, non devono muoversi. Congeliamoli, se è possibile. :-)

UNA PAROLA DIFFICILE

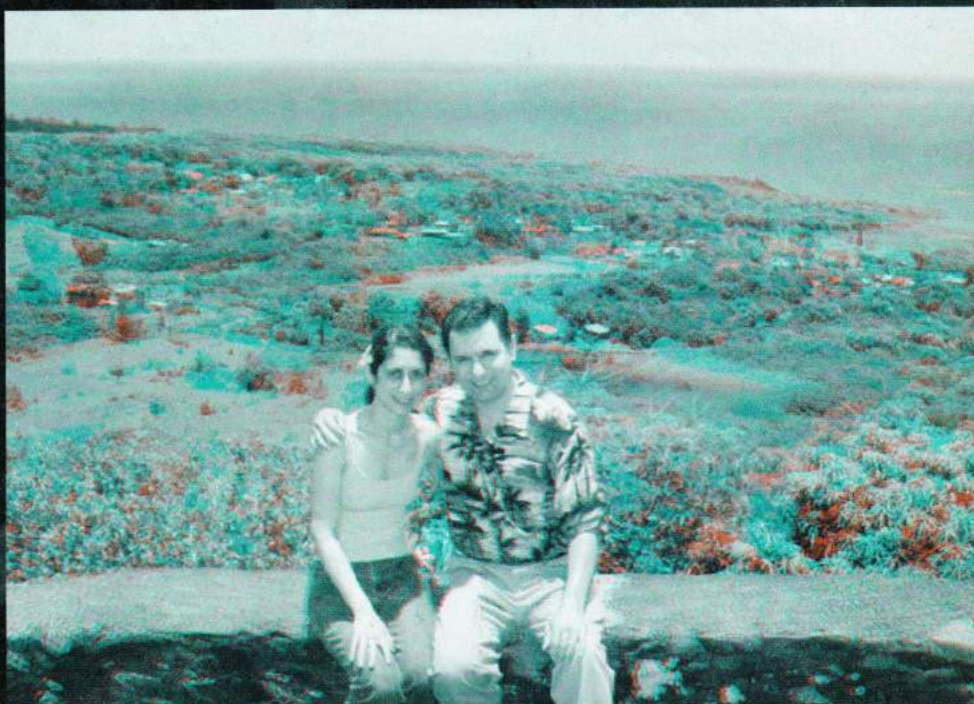
Anaglifo: Fotografia utilizzata in coppia con un'altra per produrre un effetto tridimensionale osservabile con appositi occhialini.

quelle della NASA

Fotoritocchiamo

Da Photoshop in giù, qualsiasi programma grafico che controlli i canali dei colori primari rosso, verde e blu in modo indipendente l'uno dagli altri va bene. Se proprio non abbiamo niente sottomano, si può scaricare una demo di Photoshop valida trenta giorni dal sito Adobe (http://www.adobe.com). Trasformiamo in scala di grigio entrambe le immagini. Poi prendiamo solo l'immagine sinistra e le assegnamo la modalità RGB. Ogni programma ha il suo modo di farlo. Apriamo i canali dell'immagine sinistra e selezioniamo solo i canali blu e verde.

▲ *Un'immagine viene incollata sull'altra. Una è leggermente spostata sulla destra. Devono essere allineate in orizzontale però!*

Selezioniamo ora tutto il contenuto dell'immagine destra e diamo il comando Copia. Torniamo all'immagine sinistra e diamo Incolla. Se tutto è andato bene, dovremmo vedere una immagine sfuocata blu e rossa. In alternativa, possiamo incollare avendo selezionato solo il canale blu (non blu e verde) dell'immagine sinistra.

Questa foto, vista con gli occhialini appositi, è tridimensionale!

Allineiamo

Prima di finire dobbiamo allineare meglio le immagini. Selezioniamo solo il canale rosso. Prendiamo un punto di riferimento (per esempio le pupille del soggetto) e spostiamo in su o in giù l'immagine nel canale rosso in modo che il punto di riferimento sia perfettamente allineato in orizzontale nelle due immagini. L'allineamento migliore è quello che riduce gli anelli di colore intorno alle immagini. È probabile che agli estremi dell'immagine ci siano comunque aloni consistenti. Nel caso, ritagliamo un po' i bordi per migliorare l'effetto.

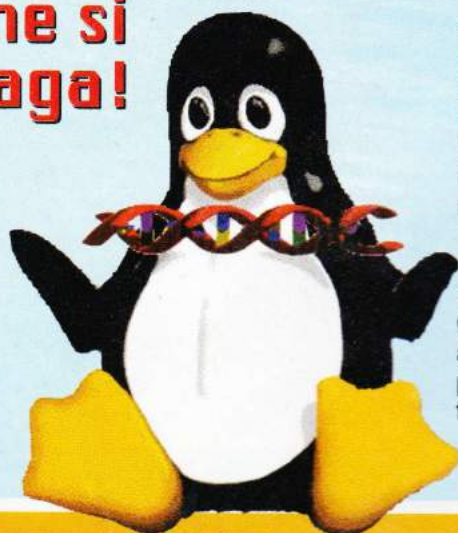
Fatto! Per vedere l'immagine, a schermo o in stampa, ci vorranno gli occhialini rossi e blu. La lente sinistra dovrebbe essere quella rossa; in caso contrario, bisogna scambiare le immagini nella procedura.

Nyarlathotep
nyarlathotep@hackerjournal.it

PROCURARSI GLI OCCHIALINI

Prima di comprare un paio di occhialini apposta per le nostre foto si può tentare di procurarsene un paio quasi gratis, acquistando un videogame che li comprende nella scatola, o conservando quelli forniti in un parco di divertimenti, o quelli in regalo in qualche rivista... ma anche fissare due pezzi di plastica colorata trasparente a un cartoncino serve allo scopo!

Trucchi e segreti per senza rischiare

Finalmente possiamo provare senza patemi il migliore sistema operativo gratuito del mondo. Migliore anche di Windows, che si paga!

Innanzitutto dobbiamo procurarci una distribuzione corretta. Sconsigliamo Slackware e Debian per la loro complicatezza; una distro [*gergo* per distribuzione. *N.d.B.*] adatta a tutti può essere Mandrake, della quale si possono trovare le immagini disco ISO su Internet.

Sono 3 CD, versione 9.2 in questo momento, scaricabili dal sito http://www.mandrakelinux.com/. Controlliamo preventivamente la compatibilità dei componenti hardware con Mandrake, a http://www.mandrakelinux.com/en/hardware.php3; se non abbiamo trovato tutto il nostro hardware, facciamo una capatina su Google, scriviamo "linux" + "nome_del_componente_hardware" e clicchiamo "Mi Sento Fortunato". I driver salteranno fuori con facilità.

Attenti al masterizzatore

Se abbiamo un masterizzatore o lettore CD/DVD marca LG leggiamo anche http://www.mandrakelinux.com/en/lgerrata.php3, perché la mdk [gergo per Mandrake. N.d.B.] potrebbe sovrascrivere il driver, quindi il lettore/masterizzatore diverrebbe inutilizzabile.

Scaricati i CD della distro, dobbiamo installarla, e abbiamo due opzioni: boot da CD o boot da floppy. Per il boot da CD dobbiamo modificare il BIOS. Stiamo attenti però a non fare stupidaggini, potrebbe costarci caro; eventualmente facciamoci aiutare da qualcuno più esperto. In alternativa, se non vogliamo

▲ *All'indirizzo http://www.mandrakelinux.com/it/ si può sapere tutto di Mandrake in lingua italiana.*

modificare il BIOS, possiamo creare un'immagine con l'utility RawWrite presente in dosutils/rawrite.exe nel CD 1 di Mandrake, digitando da MS-DOS:

```
C:\>cd D:\
D:\>dosutils\rawrite.exe -f images\cdrom.img
```

dove D:\ rappresenta il lettore CD. Facciamoci un bel backup generale, uno scandisk e un defrag, e riavviamo il computer con il floppy/CD inserito. L'installer partirà in automatico. Premiamo Invio quando verrà chiesto e attendiamo il caricamento del programma. La prima cosa da configurare è la lingua. La tappa successiva è la licenza. Leggiamola e clicchiamo su "Accetto", poi su "Avanti". Ora verrà configurato il mouse: spesso viene riconosciuto automaticamente. Se il sistema sbagliasse, indichiamogli il nostro. Facciamo magari qualche prova (cliccan-

installare LINUX Windows

▲ Basta scegliere la lingua e Mandrake si comporta benissimo anche in italiano.

do su Avanti compare una schermata dove provare il mouse).

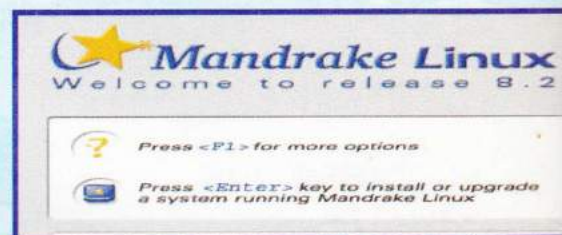
Nel prossimo passaggio impostiamo il livello di sicurezza. Per un uso personale la voce "Normale" è sufficiente. Il partizionamento, la fase successiva, è la suddivisione del disco fisso in più parti. Selezioniamo "Usa lo spazio libero della partizione Windows" e premiamo "Avanti" per ridimensionare la parte di disco fisso nella quale risiede Windows. Lasciamgli un po' di spazio libero, altrimenti andrà in crisi ad ogni minima operazione.

▲ Chi ha bisogno di Windows, se Office può essere fatto funzionare sotto Linux?

Alla pressione del tasto "Avanti" ci troviamo di fronte all'assegnazione dei punti di mount (cioè in quali partizioni si dovranno sistemare le cartelle "/" e "/home"); clicchiamo su "Avanti" poiché la configurazione standard va bene. Dopo la formattazione delle partizioni, installiamo il software e, al termine, iniziamo a configurare il sistema.

root, l'utente divino (nel bene e nel male)

Dovremo specificare la password di root, cioè dell'utente che ha il controllo completo sul sistema. Non conviene lavorare quotidianamente come root, poiché un errore fatto usando questo utente può essere irreparabile (chi scrive una volta ha usato da root il comando tee su /etc/fstab e gli è toccato reinstallare tutto…); comunque segnamoci la pass e mettiamola in un posto sicuro.

Adesso verrà creato un nuovo utente, del quale dovremo specificare nome e password, più il nome reale e l'icona. Questo utente dovrà essere usato tutti i giorni; dovremmo usare root solo in casi eccezionali, come l'installazione del software (solitamente, come user normali non abbiamo i privilegi di scrittura

▲ L'autopresentazione di Mandrake!

in /usr o altre cartelle di sistema). Poi dobbiamo scegliere il bootloader da installare, cioè il programma che ci permette di decidere quale sistema operativo avviare all'accensione del computer; infine ci troveremo davanti a una schermata di riepilogo. Ci verrà chiesto se vogliamo cercare aggiornamenti software per Internet: facciamo la nostra scelta e proseguiamo. Il sistema verrà riavviato e, da lì in poi, potremo scegliere l'OS da avviare. Buon divertimento con Linux ;-)

X-3mE'89 - HaCkInG FrOm RoOtS

▲ Non mancano neanche i giochi!

TRUCCHI da

Impariamo a capire come cercano di propinarci lo spam, per essere più bravi di loro e non farci fregare

Bene e male, guardie e ladri, spam e antispam: è una battaglia continua. Ecco come gli spammatori cercano di battere i nostri sistemi anti-posta-spazzatura.

Primo trucco: il messaggio spezzato

Riceviamo messaggi di questo tipo nelle nostre caselle ogni giorno:

▲ *Spam farmaceutico piuttosto frequente: mi hanno quasi convinto di averne bisogno :-(*

Adesso guardiamo l'HTML che sta dietro il messaggio (abbiamo tagliato un po' di codice non rilevante):

```
<html>
<body>
<center>
 <font face="Arial" size="5">
 <table cellspacing=0 cellpadding=0
border=0 width=550> <tr>
  <td align=right>
  <table cellspacing=0 cellpadding=0
border=0 width=200>
   <tr>
    <td align=right>Hel<br>
    <br></td>
   </tr>
   <tr>
    <td align=right> <b>Get <a
href="http://">G-E-N-E-R-I-C V-
I</a></b><br>
    <br> </td>
   </tr>
   <tr>
    <td align=right> <b>Follow <a
href="http://">t</a></b> </td>
   </tr>
  </td>
  </tr>
  </table>
 </td>
 <td>
  <table cellspacing=0 cellpad-
ding=0 border=0 width=300>
   <tr>
    <td>lo!<br>
    <br></td>
   </tr>
   <tr>
    <td><b><a href="http://">-A-G-
R-A</a> from the Best One!</b><br>
    <br></td>
   </tr>
   <tr>
    <td><b><a href="http://">his
link!</a></b></td>
   </tr>
  </td>
  </tr>
  </table>
 </td>
 </tr> <tr>
  <td align=left><br>
   <br>
     B
est Wishes!</td>
  </tr>
 </table>
</center>
</font> <br>
<br>
</body>
</html>
```

Capito il trucco? Il messaggio è spezzato e inserito in celle di tabelle. Proviamo a sostituire nel codice border=0 con border=1 e tutto diventa più chiaro:

▲ *Ora si vedono le tabelle in cui è stato spezzato il testo, per ingannare i filtri antispam.*

Non è facile filtrare questa roba. L'unico modo è disporre di un antispam capace di analizzare non solo il codice HTML ma anche la sua resa finale nel browser.

Secondo trucco: l'immagine dentro

Capiterà assai di rado che un amico ci mandi un messaggio in HTML contenente link a immagini esterne (con un link come <img src="http:…">). Quindi filtrare questo tipo di link tiene lontano un bel po' di immondizia. Ma ci sono anche i messaggi che fanno finta di tenere immagini dentro il codice e invece non è vero. Occhio a questo HTML:

```
<HTML>
<body>
<base href="http://indirizzo.dello/spam-
mer/">
...
<IMG SRC="p1_01.gif" border=0>
...
</body>
</HTML>
```

A guardare il tag <IMG…> sembra una innocente immagine interna. Ma il tag <base…> fa sì che invece il link punti da qualche altra parte, chissà dove. Questo trucco si applica a tutti i tipi di link e una soluzione abbastanza facile consiste nel filtrare i messaggi che contengono il tag <base> su cui si… basa l'inganno.

Terzo trucco: bianco sporco

Partiamo subito dal codice truccato:

```
<html>
<body bgcolor="#FFFFFF">
<font color="#FFFFCC">Abbocca al nostro spam nascosto!</font>
<br>
Vuoi vincere un milione di euro alla lotteria? Clicca <a href="http://www.sitoqualunque.com">qui</a>
</body>
</html>
```

Nel browser si vedrà solo la seconda frase: la prima infatti è in bianco su bianco. Noi abbiamo riportato una frase banale, ma uno spammer vero userebbe il trucco per inserire parole senza senso che portino fuori strada le nostre statistiche antispam. Si può vedere la frase incriminata se selezioniamo il testo. Evidenziandolo, apparirà anche la parte bianca.

Vuoi vincere un milione di euro alla lotteria? Clicca qui

▲ *Una frase qualunque, in un messaggio innocente…*

Sembra che la soluzione ovvia sia filtrare il testo di colore bianco, ma bisogna stare attenti. Noi stessi, nell'esempio, abbiamo usato un quasi-bianco, codice FFFFCC, che comunque sullo sfondo bianco-bianco (FFFFFF) non si nota comunque. Quindi sono da filtrare le tonalità del bianco e non solo il bianco puro.

Abbocca al nostro spam nascosto!
Vuoi vincere un milione di euro alla lotteria? Clicca qui

▲ *…ma selezionando il messaggio ci si accorge di contenuto nascosto, bianco o quasi bianco su fondo bianco.*

OFFUSCARE IL CODICE

Nascondere lo spam dentro il codice HTML discende direttamente dall'arte di offuscare il codice, ossia di scrivere un programma in modo che un osservatore non possa vedere che cosa fa il programma stesso solo guardando il sorgente. Per esempio, che cosa fa il programma in C riportato qui sotto?

```
#define D define
#D Y return
#D R for
#D e while
#D I printf
#D l int
#D C y=v+111;H(x,v)*y++= *x
#D H(a,b)R(a=b+11;a<b+89;a++)
#D s(a)t=scanf("%d",&a)
l V[1100],u,r[]={-1,-11,-10,-
9,1,11,10,9},h[]={11,18,81,88},ih[]={22,27,
72,77},bz,lv=60,*x,*y,m,t;S(d,v,f,a,b)l*
v;{lc=0,*n=v+100,bw=d<u-1?a:-
9000,w,z,i,zb,q=3-
f;if(d>u){R(w=i=0;i<4;i++)w+=(m=v[h[i]]
)==f?300:m==q?-300:(t=v[ih[i]])==f?-
50:t==q?50:0;return
w;}H(z,0){if(GZ(v,z,f,100)){c++;w= -
S(d+1,n,q,-b,-
bw);if(w>bw){zb=z;bw=w;if(w>=b||w>
=8003)Yw;}}}if(!c){bz=0;C;Y-S(d+1,n,q,-
b,-bw);}bz=zb;Yd>=u-
1?bw+(c<<3):bw;}main(){R(;t<1100;t+=1
00)R(m=0;m<100;m++)V[t+m]=m<11||m
>88||(m+1)%10<2?3:0;V[44]=V[55]=1;V[
45]=V[54]=2;I("Level:");s(u);e(lv>0){do
{I("Yo\
u:");s(m);}e(!GZ(V,m,2,0)&&m!=99);if(
m!=99)lv-
;if(lv<15&&u<10)u+=2;I("Wait\n");I("V
alue:%d\n",S(0,V,1,-
9000,9000));I("move: %d\n",(lv-
=GZ(V,bz,1,0),bz));}}GZ(v,z,f,o)l*v;{l*j,q
=                    3                    -
f,g=0,i,h,*k=v+z;if(*k==0)R(i=7;i>=0;i-
){j=k+(h=r[i]);e(*j==q)j+=h;if(*j==f&&j
-h!=k){if(!g){g=1;C;}e(j!=k)*((j-
=h)+o)=f;}}Y g;}
```

Quarto trucco: il ridirigibile

In quest'ultimo trucco – per stavolta – il messaggio HTML sembra pulito, ma nell'intestazione si nasconde una riga minacciosa:

```
meta http-equiv="refresh" content="0;URL=http://casa.di.uno.spammer">
```

Appena apriamo il messaggio in un client di posta abilitato all'HTML, veniamo immediatamente ridiretti verso il sito dello spammer. La soluzione consiste nel filtrare il meta tag refresh, che difficilmente apparirà in una mail amica.

Chi conosce altri trucchi può mandarli alla redazione; verranno pubblicati.

Michele Campovecchio
michele_c@hackerjournal.it

Questo programma gioca a Reversi (o Othello). Per motivi di spazio non disegna la scacchiera e ha un finale di partita piuttosto debole, ma non è male per essere così piccolo. All'inizio chiede un livello di gioco, da 0 a 10, e poi la prima mossa. La mossa è un numero da 11 a 88 (11 = riga 1, colonna 1), oppure 99 per passare.

WINDOWS SENZA DISCO

C'è chi è riuscito a usare e rendere stabile un PC senza disco rigido con Windows 98. Ecco le spiegazioni e a che cosa ci può servire.

I vantaggi di un disco RAM? Velocissimo!

Gli svantaggi? Un problema e perdiamo tutto il lavoro

▲ Windows 98 in modalità diskless è molto praticato nei Paesi dell'estremo Oriente

Ci sono tante situazioni in cui fa comodo avere una stazione di lavoro che non richieda di lavorare sul disco rigido. In tutti i casi non è una cosa semplice, perché i nostri sistemi operativi sono concepiti per accedere al disco spesso e volentieri. Ecco come si può mettere a punto un computer con Windows 98 in modo che funzioni senza disco rigido.

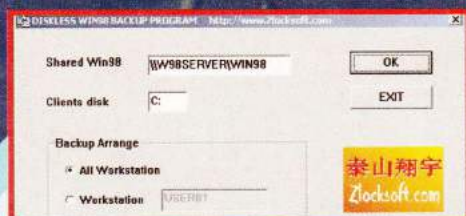
Il disco virtuale

Il trucco sta tutto nel fare funzionare Windows in una zona di RAM che viene trattata dal sistema come se fosse un piccolo disco rigido. Si tratta di una tecnica piuttosto in voga anni fa, quando i dischi rigidi costavano molto più di ades-

ALCUNI SITI PER IL PEER-TO-PEER

Netboot 0.9.8
http://netboot.sourceforge.net
Permette di creare l'immagine disco che poi verrà montata nel disco RAM dal server remoto.

Etherboot 5.2
http://etherboot.sourceforge.net/
Alternativa a Netboot per creare l'immagine disco di cui sopra.

ODI/VLM
ftp://ftp.parked.com/pub/vlmkt6.exe
Shell per copiare l'immagine disco tra server di rete e disco RAM

▲ *Ci sono anche programmi commerciali, come RPL Diskless Windows 98, che facilitano enormemente la messa a punto di un sistema diskless.*

so ed erano lenti. I vantaggi: Windows va velocissimo! Gli svantaggi: un errore di sistema, o un millisecondo di blackout, e tutto il lavoro fatto (che sta in RAM) va perso.

In pratica

Installiamo Windows 98 sul disco rigido e poi comprimiamo l'installazione con ms-drvspace3, operazione che crea un file nascosto chiamato drvspace.000 Questo file può essere copiato su un disco RAM e poi montato come disco C: mediante il comando scandisk C: /mount.

Se ci troviamo su una rete, è anche possibile mettere parti del filesystem di Windows 98 su un server remoto. Naturalmente si crea un problema di velocità di trasmissione, perché l'esecuzione della copia di Windows compressa è più lenta del normale e, se è lenta anche la rete, è la fine. Assicuriamoci di avere banda in abbondanza e RAM in abbondanza per evitare problemi di lentezza.

Poiché al momento del boot la rete non è ancora disponibile, il file di swap dovrà trovarsi in locale (e sarà anche lui compresso).
Ecco i passi per effettuare la procedura:

A) installiamo Windows 98 sul disco locale (installazione standard);
B) comprimiamo il disco locale usando la compressione più efficace a disposizione;
C) terminata la compressione, copiamo il file nascosto drvspace.000 dalla radice del disco non compresso su un file server di rete;
D) creiamo un floppy disk di boot di Windows;
E) copiamo sul floppy la shell e tutti i file necessari. I file config.sys e autoexec.bat vanno sistemati in modo da:
- Caricare il disco RAM (in config.sys)
- Caricare shell e login (come shell noi abbiamo usato ODI/VLM, ma va bene qualunque altra shell adatta)
- Copiare drvspace.000 dal server di rete al disco RAM
- Chiudere la shell
- Montare il volume compresso
- Avviare Windows

F) copiare il filesystem che sta su floppy disk in un file, usando dd o altro programma in grado di spostare i dati in forma grezza. Questo passo è indispensabile per poter creare una immagine che possa eseguire il boot via rete;
G) usare il comando mknbi-dos di Net-Boot per creare una immagine di boot;
H) vedere se funziona (nel dubbio, scollegare fisicamente il disco rigido); se ci sono problemi (dipende dal computer e dai programmi usati) modificare la configurazione per un nuovo tentativo.

▲ *Se si fanno le cose sul serio, si possono usare sistemi diskless anche con più volumi, montati su altrettanti volumi di rete.*

TROPPO DIFFICILE? BASTA PAGARE

Questo articolo non è alla portata di tutti e richiede una certa conoscenza di Windows. Ci raccomandiamo di non fare danni al computer se non sappiamo dove e come mettere le mani, o se non siamo disposti a correre il rischio di una reinstallazione.

Esistono vari pacchetti che consentono di usare Windows in modo diskless senza dover essere amministratori di sistema competenti.

Uno di questi è, per esempio, RPL Diskless Windows 98 di Zlocksoft, reperibile a **http://www.zlocksoft.com/english/diskless98.htm.**

Costa 88 dollari e si può ordinare direttamente dal sito, avendo una carta di credito.

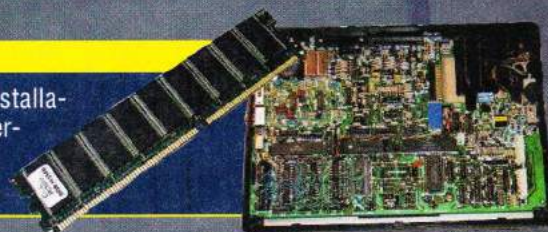
```
Windows

A fatal exception 0E has occurred at 0028:C0011E36 in UXD UMM(01) +
00010E36. The current application will be terminated.

*  Press any key to terminate the current application.
*  Press CTRL+ALT+DEL again to restart your computer. You will
   lose any unsaved information in all applications.

                    Press any key to continue _
```

Un computer che usa Windows senza accedere al disco rigido va velocissimo, ma un errore come questo fa perdere tutto il lavoro fatto...

DELLE DIFFICOLTÀ DI METTERE WINDOWS IN UN DISCO RAM

Ci possono essere problemi di dimensioni, perché non tutti i dischi RAM disponibili per Windows riescono a gestire spazi grandi abbastanza per fare funzionare Windows. In caso di difficoltà semplifichiamo il più possibile l'installazione di Windows togliendo tutto il superfluo che riusciamo.

IL PROSSIMO NUMERO

IL 3 giugno 2004!

CYBERENIGMA

Abbiamo messo le mani su un documento di vent'anni fa. Sono gli aiuti per risolvere il primo gioco di avventura in italiano, creato prima per Apple II e poi per tutti gli altri sistemi operativi. Gli aiuti, per non dare subito la soluzione, erano cifrati e per leggerli serviva questo programma decodificatore:

```
10    INPUT "CODICE";CC:PRINT "SCRIVI: ";
20    GET C$:IF C$="" THEN 20
30    IF C$=CHR$(13) THEN END
40    C=ASC(C$)
50    IF C>=65 THEN C=C+CC:IF C>90 THEN C=C-26
60    PRINT CHR$(C);
70    GOTO 20
```

Questi sono tre frammenti degli aiuti:

Contenuto pergamena: (25)
EJBHOPTJ: JM TPHHFUUP QBSF BGGFUUP EB HSBWF DBSFOAB EJ TFOOP. UFSBQJB DPOTJHMJBUB: EVF GMBDPOJ EJ GVSCPMJOB BM HJPSOP QFS TFJ NFTJ, F QFS FTFSDJAJP TDSJWFSF MB QBSPMB VOB MFUUFSB BMMB WPMUB.

Diamante: (13)
TYV NAGVPUV CEBIREOV PBAGRATBAB FCRFFB ZBYGN FNTTRMMN. VA CNEGVPBYNER AR PBAGVRAR DHRYYB PUR GEBIV ARYYN FGNAMN QRYYN CEVAPVCRFFN.

Parola magica: (20)
NGO UYYKXBGZU ZAZZU TKRRG YZGTFG JKRRK IURUTTK? (BKJO)

✪ **Per tutti:** che cosa c'è scritto?

✪✪ **Per esperti:** in che linguaggio è scritto il decodificatore? Come funziona?

✪✪✪ **Per geni:** sai scrivere lo stesso programma in un altro linguaggio?

✪✪✪✪ **Per super hacker:** sai scrivere il programma codificatore, che parte dalle frasi in chiaro e crea la cifratura? Di che gioco si tratta? Riesci a trovarne traccia su Internet?

Alla prossima!